Serial No.: 09/705,998

1   On page 48, replace the emboldened heading on the top of the page under the title with:

2   ABSTRACT

3   On page 48 replace the abstract with the following paragraph:

4   The present invention provides encryption schemes and apparatus which securely

5   generate a cipher-text which in itself contains checks for assuring message integrity. It

6   also provides compatible decryption schemes confirming message integrity. The

7   encryption scheme generates a cipher-text with message integrity in a single pass with

8   little additional computational cost, while retaining at least the same level of security as

9   schemes based on a MAC. One embodiment encrypts a plain-text message by dividing

10   the plain-text message into a multitude of plain-text blocks and encrypting the plain-text

11   blocks to form a multitude of cipher-text blocks. A single pass technique is used in this

12   process to embed a message integrity check in the cipher-text block. A message integrity

13   check is embedded in the cipher-text blocks by embedding a set of pseudo random

14   numbers, which may be dependent, but are pair-wise differentially uniform. We also

15   describe an embodiment which is highly parallelizable .

16

DOCKET NUMBER: YOR920000763US1   -4/34-